What is claimed is:

Sub a1

1. A monitoring device disposed for thwarting denial of service attacks on the data center, the monitoring device comprising:

a plurality of probe devices that are disposed to collect statistical information on packets that are sent between the network and the data center;

a cluster head coupled to each of the plurality of probe devices, the cluster head receiving collected statistical information from the probe devices and determining from the collected information whether the data center is under a denial of service attack.

2. The device of claim 1 wherein the cluster head is coupled to the plurality of probe devices through a dedicated, private network.

3. The device of claim 2 wherein the cluster head further comprises:

a communication process that communicates statistics collected in the probe devices with a control center, and that receives queries or instructions from the control center.

4. The device of claim 3 wherein the monitoring device is a gateway device and further comprises:

a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

5. The device of claim 1 wherein the probes are physically deployed in line in the network.

6. The device of claim 1 wherein the probes execute a joining process that allows a probe to join a cluster.

7. The device of claim 1 wherein the cluster head comprises a process to aggregate traffic from the various probes and to produce logs and apply detection heuristics.

8. A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

monitoring network traffic through probes that are disposed between the victim data center and the network; and

communicating data from the probes, over a dedicated network, to a cluster head device.

9. The method of claim 8 further comprising:

communicating data from the cluster head device to a control center over a hardened network.

10. The method of claim 8 further comprising:

analyzing network traffic statistics to identify malicious network traffic; and

filtering network traffic, which is identified as malicious network traffic, during analyzing of the network traffic.

11. The method of claim 8 wherein the cluster head device and the probe devices comprise a clustered gateway.

12. The method of claim 11 wherein when a new cluster probe is added to the clustered gateway, the method further comprises:

dynamically discovering the new cluster probe that seeks to join the cluster.

13. The method of claim 8 further comprising:

performing intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate the malicious traffic.

14. The method of claim 13 wherein performing intelligent traffic analysis is controlled by the cluster head and filtering is performed by the probes.

15. A gateway for thwarting denial of service attacks on a victim comprises:

a cluster head; and

a plurality of probes disposed between a network and a victim, the probes collecting statistical data, for performance of intelligent traffic analysis and filtering by the probed, to identify malicious traffic for thwarting denial of service attacks.

16. The gateway of claim 15 wherein the gateway includes a process to insert filters to discard packets that are deemed to be part of an attack.

17. A monitoring device disposed for thwarting denial of service attacks on the data center, the monitoring device comprising:

a device that collects statistical information on packets that are sent between the network and the data center over a plurality of links and that produces statistical information from network traffic over the plurality of links to determine from the statistical information whether the data center is under a denial of service attack.

18. The monitoring device of claim 17 wherein the monitoring device is coupled to a control center through a hardened network.

19. The monitoring device of claim 17 wherein the device further comprises:

a communication process that communicates statistics with a control center, and that receives queries or instructions from the control center.

20. The monitoring device of claim 17 wherein the monitoring device is a gateway device and further comprises:

a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

21. The monitoring device of claim 20 wherein the gateway comprises:

a process to aggregate traffic from the various links and to produce logs and detection heuristics.

22. A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

monitoring network traffic over a plurality of links between the victim data center and the network; and

communicating data, over a hardened network, to a control center.

23. The method of claim 22 wherein monitoring is performed by probe devices that sample network traffic at a constant rate.

24. The method of claim 23 wherein the sampled network traffic by the probes is delivered to a clustered head for traffic analysis.

25. The method of claim 23 wherein the probes send the sampled network traffic to the cluster head at a substantially constant rate irrespective of traffic on the monitored network.